Status of the Claims

Claims 1 - 32 are pending.*

Claims 1 – 32 stand rejected.*

Argument.

Claims 1 – 8, 10, 12 – 19, 21 – 29 and 31 - 32 stand rejected under 35 U.S.C. 102(b) as being anticipated by Matsui (United States Patent No. 5,488,661).* Claims 9, 20 and 30 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Matsui in view of McNair (United States Patent No. 4,642,424). Claim 11 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Matsui in view of Neimat (United States Patent No. 5,542,087). Applicant respectfully requests reconsideration and removal of these rejections for at least the following reasons.

I. Summary

For purposes of explanation only, the present application teaches a method of encrypting a data message consisting of a plurality of data message blocks before transmitting those data message blocks over a network. This is accomplished by extracting a data value from one of the message data blocks and selecting an encryption key from among a plurality of encryption keys dependently upon the extracted data value. A subsequent one of the message data blocks is then encrypted using the selected encryption key.

* Applicant notes Claim 21 was cancelled in the previous Amendment mailed December 22, 2004.

In this manner, a party will transmit a message block that is encrypted using an encryption key determined from the data content of a previously transmitted message block. *See, e.g., page 5, third full paragraph.* Further, the data content of a last message data block is used to determine the encryption key selected to transmit a current message data block. *See, e.g., page 6, first full paragraph.*

In contrast, Matsui teaches determining a plurality of encryption keys for a fixed number of input data bytes based upon manipulation of those very same input data bytes, and not upon any previously received information, and clearly not upon a previously received message data block to be transmitted over a network.

II. Discussion

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *See, M.P.E.P. §2131 citing Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).* That is, "the identical invention must be shown in as complete detail as is contained in the. . . claim." *Richardson v. Suzuki Motor Co., 9 USPQ.2d 1913, 1920 (Fed. Cir. 1989) (emphasis added).* Applicant respectfully submits Matsui fails to teach each and every element found in any of the independent Claims 1, 13 or 24 – and hence, as a matter of law fails to anticipate any of these claims. For purposes of completeness, Applicant submits McNair and Neimat fail to remedy the shortcomings of Matsui, and hence fail, in any combination, to render any of the present claims unpatentable.

A. Claims 1 - 12.

Claim 1 recites encrypting a subsequent message block using a key selected dependently upon a previous message block. Matsui teaches dividing a message or data block into more and less significant portions, and encrypting that message using keys selected from the less significant portions. Matsui's use of portions of a data block to select encryption keys for that very same data block does not anticipate the claimed use of data extracted from a previous block to select a key for encrypting a subsequent block.

This shortcoming is evident in the Final Office action mailed December 22, 2004, wherein it is argued that:

> "Matsui teaches that a second processing block encrypts a second input data by using a key selected dependently upon the 4 less significant bits of the previous processing block's output (Matsui, column 6 lines 17-35)." *See 4/15/2005 Office action, par. 4, lines 6-9.*

However, a detailed reading of Matsui reveals that the process disclosed therein concerns encrypting an 8 byte data block using data extracted from *that very same data block* to determine an encryption key. Thus, Matusi does not anticipate encrypting a *subsequent message data block* using a key determined on the basis of data extracted from a *previous message data block.* While Matsui refres to *processing blocks*, such processing blocks or steps cannot be read onto the claimed message data blocks.

By way of further explanation, Claim 1 recites:

> A method to encrypt a data message having a plurality of message data blocks prior to transmitting said message data blocks over a network, said method comprising:
>
> extracting a data value from one of said message data blocks;
>
> selecting an encryption key from among a plurality of encryption keys dependently upon said extracted data value; and,

> encrypting a subsequent one of said message data blocks using said selected encryption key.

In rejecting Claim 1, the Final Office action argues

> "Matsui teaches the extracting of a data value from a message data block (Matsui, column 5 line 67 - column 6 line 4, selects less significant 4 bytes)."

The Final action further argues

> Matsui teaches "selecting of an encryption key from among a plurality of encryption keys dependently upon said extracted data value (Matsui, column 6 lines 17 - 35, extended key), [and] encrypting a subsequent message data block using the selected encryption key (Matsui, column 6 lines 17-35).

Applicant traverses these assertions. A detailed reading of the above-cited passages reveals that Matsui inputs a single data block (e.g., the 8 bytes of plaintext designated numeral 3 in Fig. 1), and divides this single data block into more and less significant portions (e.g. the 4 more and 4 less significant 4 bytes) of that same data block. *See, e.g., U.S. Patent No. 5,488,661, col. 5, line 67 – col. 6, line 1.* Matsui calculates an address based upon the less significant bytes portion of the single plaintext message block 3. *See, e.g., U.S. Patent No. 5,488,661, col. 6, lines 4- –7.* Matsui then supplies a key selected using the calculated address to a first processing block 9. *See, e.g., U.S. Patent No. 5,488,661, col. 6, lines 7 – 9.* Processing block 9 of Matsui uses the scrambling key to scramble the same less significant byte portion that was used to calculate the address, and hence select the scrambling key in the first place. *See, e.g., U.S. Patent No. 5,488,661, col. 6, lines 10 - 13.*

Matsui then exclusive ORs the scrambled least significant portion with the more significant portion of the single input message block. *See, e.g., U.S. Patent No.*

5,488,661, col. 6, lines 13 - 14. Finally, the resultant and less significant portion replace one another. *See, e.g., U.S. Patent No. 5,488,661, col. 6, lines 15 - 67 – col. 6, lines 14 - 16.*

The output, consisting of the calculated result (based upon XORing the more and scrambled less significant byte portions) and the less significant byte portion of the single input data block is input to the second block 10 (see, e.g., Fig. 2, where the single 2 byte input data block includes 1 more significant byte (00) and 1 less significant byte (00), and processing block 10 receives (FF), (00) from processing block 9). *See, e.g., U.S. Patent No. 5,488,661, col. 6, line 66 – col. 7, line 1.* Scrambling block 10 uses the output of block 9 in an analogous manner to provide an output to processing block 11, which operates in an analogous manner to provide an output to processing block 12, and so on.

<u>Eventually, in response to a single 8 byte plaintext input data block 3, Matsui provides a single 8 byte scrambled output data block 4</u>. *See, e.g., U.S. Patent No. 5,488,661, Figs. 1 and 2; col. 5, lines 44 - 46.*

In view of the foregoing, it is clear that Matsui merely teaches <u>*using a sequence of processing blocks*</u> *(e.g., 9 – 16)* to scramble a <u>*single input data block*</u> 3 using keys ultimately selected on the basis of that very <u>*same single input data block*</u> (e.g., the 4 less significant bytes in the single message block at the corresponding processing block). Matsui does <u>not</u> teach scrambling a future input data block 3 using some value extracted from the present input data block 3 – as each data input 3 is scrambled solely on the basis of its own data values.

In contradistinction to the teachings of Matsui, Claim 1 clearly recites extracting a data value from one of said message data blocks; selecting an encryption key from among a plurality of encryption keys dependently upon said extracted data value; and, encrypting a *subsequent one of said message data blocks* using said selected encryption key. Put another way, the Matsui reference merely teaches an encryption scheme that uses *intra*-data block processing key selection. Accordingly, Matsui clearly fails to teach the claimed *inter*-message data block dependent key selection recited in present claim 1.

In view of the foregoing reasons, Applicant respectfully requests reconsideration and removal of the rejection of Claim 1. Applicant further requests reconsideration and removal of the rejections of Claims 2 – 12 as well, at least by virtue of these claims' ultimate dependency upon a patentably distinct base Claim 1.

B. Claims 13 – 20, 22 and 23

In similar fashion to that of Claim 1, present Claim 13 recites

> A system for selecting at least one encryption key used to encrypt a data message having a plurality of message data block prior to transmitting said message blocks over a network, said system comprising:
>
> a communication apparatus operative to:
>
> extract a data value from one of said message data blocks;
>
> select an encryption key from among a plurality of encryption keys stored in a memory dependently upon said extracted data value; and,
>
> encrypt at least a subsequent one of said message data blocks using said selected encryption key.

Accordingly, Applicant also respectfully requests reconsideration and removal of the rejection of Claim 13 for at least the foregoing reasons. Applicant also respectfully requests reconsideration and removal of the rejections of Claims 14 – 20 and 22 - 23 as well, at least by virtue of these claims' ultimate dependency upon a patentably distinct base Claim 13.

C. Claims 24 - 32.

Independent Claim 24 similarly recites:

> A device for use with a plurality of encryption keys stored in a memory, and useful for encrypting a message composed of data message blocks, said device comprising:
>
> a processor, in communication with said memory, operative to:
>
> extract a known number data bits from one of said data message blocks;
>
> select an encryption key from said stored encryption keys based on the content of said extracted data bits; and
>
> encrypt a subsequent one of said data message blocks using said selected encryption key;

Accordingly, Applicant also respectfully requests reconsideration and removal of the rejection of Claim 24 for at least the foregoing reasons. Applicant also respectfully requests reconsideration and removal of the rejections of Claims 25 – 32 as well, at least by virtue of these claims' ultimate dependency upon a patentably distinct base Claim 24.

III. Conclusion

Wherefore, Applicant believes he has addressed all outstanding grounds raised in the outstanding Office action, and respectfully submits the present case is in condition for allowance, early notification of which is earnestly solicited.

Should a notice of allowance not be forthcoming, Applicant respectfully requests this amendment be entered for purposes of preparing the record for appeal.

Should there be any questions or outstanding matters, the Examiner is cordially invited and requested to contact Applicant's undersigned attorney at his number listed below.

Respectfully submitted,

Edward J. Howard
Registration No. 42,670

Plevy, Howard & Darcy, P.C.
PO Box 226
Fort Washington, PA 19034
Tel: (215) 542-5824
Fax: (215) 542-5825